The listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claim 1 (currently amended) A method for providing gated access for a third party to a secure entity or service comprising ~~the steps of~~:

storing biometric data in dependence upon a biometric characteristic of a first designated user of the secure entity or service other than the third party;

capturing biometric information representative of a biometric characteristic and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data to produce a comparison result; and,

if the comparison result is indicative of a match:

providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service said access provided for a predetermined, limited period of time.

Claim 2. (currently amened) A method of providing gated access for a third party to a secure entity or service as defined in claim 1, comprising ~~the steps of~~:

receiving the gating signal at the secure entity or service;

in response to the wireless gating signal, setting a flag within the secure entity or service, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the secure entity or service is non responsive to the wireless signals and in a second other state the secure entity or service is responsive to the wireless signals provided by the third party.

Claim 3 (original) A method for providing gated access for a third party to a secure entity or service as defined in claim 2, wherein the flag is returned to the first state after a predetermined amount of time.

Claim 4 (currently amended) A method for providing gated access for a third party to a secure entity or service comprising ~~the steps of~~:

storing biometric data in dependence upon a biometric characteristic of a first designated user of the secure entity or service other than the third party;

storing [[toring]] biometric data in dependence upon a biometric characteristic of the third party;

capturing biometric information representative of a biometric characteristic and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data of the first designated user to produce a comparison result; and,

if the comparison result is indicative of a match:

providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service;

receiving the gating signal at the secure entity or service; and,

in response to the wireless gating signal, setting a flag within the secure entity or service, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the secure entity or service is non responsive to the wireless signals and in a second other state the secure entity or service is responsive to the wireless signals provided by the third party, the flag supporting a timing function such that the flag once set to the second other state returns to the first state after a predetermined, limited period of time absent additional comparison results indicative of a match.

Claim 5 (currently amended) A method for providing gated access for a third party to a secure entity or service as defined in claim 4, comprising ~~the steps of~~:

capturing biometric information representative of the biometric characteristic of the third party and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data of the third party to produce a comparison result; and,

if the comparison result is indicative of a match:

providing a wireless signal to the secure entity or service.

Claim 6 (currently amended) A method for providing gated access for a third party to a secure entity or service as defined in claim 5, comprising ~~the step of~~ providing access to the secure entity or service by the third party if the flag is in the second other state.

Claim 7 (original) A method for providing gated access for a third party to a secure entity or service as defined in claim 5, wherein the third party comprises a plurality of persons.

Claim 8 (original) A method for providing gated access for a third party to a secure entity or service as defined in claim 7, wherein different persons of the plurality of persons have different predetermined access privileges.

Claim 9 (original) A method for providing gated access for a third party to a secure entity or service as defined in claim 8, comprising a plurality of different wireless signals associated with different persons of the third party having different access privileges.

Claim 10 (original) A method for providing gated access for a third party to a secure entity or service as defined in claim 8, wherein the different predetermined access privileges comprise functional limitations of the secure entity or service.

Claim 11 (currently amended) A method for providing gated access for a third party to a secure entity or service comprising ~~the steps of~~:

providing to a first designated user other than the third party a first portable biometric device operable to capture biometric information presented thereto, the portable biometric device having stored biometric data in dependence upon a biometric characteristic of the first designated user;

providing the third party with a second other portable biometric device operable to capture biometric information presented thereto, the second portable biometric device having stored biometric data in dependence upon a biometric characteristic of the third party;

capturing biometric information representative of a biometric characteristic in response to the first designated user presenting said information to the first portable biometric device and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data in the first portable biometric device to produce a comparison result; and,

if the comparison result is indicative of a match, performing ~~the steps of~~:

providing a wireless gating signal from the first portable biometric device for enabling wireless signals provided by the third party to access the secure entity or service;

receiving the gating signal at a port of the secure entity or service; and,

in response to the wireless gating signal, setting a flag within a locking mechanism of the secure entity or service, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the locking mechanism is non responsive to the wireless signals and in a second other state the locking mechanism is responsive to the wireless signals provided by the third party.

Claim 12 (currently amended) A method for providing gated access for a third party to a secure entity or service as defined in claim 11, comprising ~~the steps of~~:

capturing biometric information representative of a biometric characteristic in response to the third party presenting said information to the second portable biometric device and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data in the second portable biometric device to produce a comparison result;

if the comparison result is indicative of a match, performing ~~the steps of~~:

capturing biometric information representative of the biometric characteristic of the third party and providing biometric data in dependence thereupon;

comparing the captured biometric data with the stored biometric data of the third party to produce a comparison result; and, if the comparison result is indicative of a match:

transmitting a wireless signal from the second portable biometric device to a port of the secure entity or service.

Claim 13 (currently amended) A method for providing gated access for a third party to a secure entity or service as defined in claim 12, comprising ~~the step of~~ providing access to the secure entity or service by the third party if the flag is in the second other state.

Claim 14 (original) A method for providing gated access for a third party to a secure entity or service as defined in claim 12, wherein the wireless gating signal from the first portable biometric device and the wireless signal from the second portable biometric device are received at different ports of the secure entity or service.

Claim 15 (original) A security system for securing an entity or a service from indiscriminate access and for providing gated access for a third party, the security system comprising:

at least a portable biometric device, the device comprising:

a biometric sensor for capturing biometric information representative of a biometric characteristic in response to a person presenting said information to the portable biometric device;

an encoder for digitally encoding the captured biometric information and providing biometric data in dependence thereupon;

memory for storing biometric data indicative of a biometric characteristic of a first designated user;

a processor for comparing the captured biometric data with stored biometric data to produce a comparison result, and if the comparison result is indicative of the first designated user for providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service, and if the comparison result is indicative of the third party for providing a wireless signal; and, a transmitter for wireless transmission of the wireless gating signal or the wireless signal;

at least a port for receiving the wireless gating signal and the wireless signal from the portable biometric device; and,

a locking mechanism for securing the entity or service, the locking mechanism comprising a processor for setting a flag in response to the wireless gating signal, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the locking mechanism is non responsive to the wireless signals and in a second other state the locking mechanism is responsive to the wireless signals provided by the third party.

Claim 16 (original) A security system for securing an entity or a service from indiscriminate access as defined in claim 15, wherein the portable biometric device comprises memory for storing biometric data indicative of a biometric characteristic of the third party.

Claim 17 (original) A security system for securing an entity or a service from indiscriminate access as defined in claim 16, wherein the security system comprises a first portable biometric device for use by the first designated user and a second other portable biometric device for use by the third party.

Claim 18 (original) A security system for securing an entity or a service from indiscriminate access as defined in claim 15, wherein the biometric sensor comprises a fingerprint imager.

Claim 19 (original) A security system for securing an entity or a service from indiscriminate access as defined in claim 18, wherein the fingerprint imager comprises a capacitive fingerprint imager.

Claim 20 (original) A security system for securing an entity or a service from indiscriminate access as defined in claim 15, wherein the locking mechanism comprises memory for storing data indicative of access privileges.